

NSW AI Operational Policy

Final version 1: July 2026



Acknowledgement of Country

The Department of Customer Service acknowledges the Traditional Custodians of the lands where we work and live. We celebrate the diversity of Aboriginal peoples and their ongoing cultures and connections to the lands and waters of NSW.

We pay our respects to Elders past, present and emerging and acknowledge the Aboriginal and Torres Strait Islander people that contributed to the development of this document.

NSW AI Operational Policy

Published by Digital NSW within the Department of Customer Service.

<https://www.digital.nsw.gov.au>

First published: July 2026.

More information

Contact the NSW Office for AI via email at oai@customerservice.nsw.gov.au.

Copyright and disclaimer

© State of New South Wales through the Department of Customer Service 2026. Information contained in this publication is based on knowledge and understanding at the time of writing, July 2026, and is subject to change. For more information, please visit <https://www.nsw.gov.au/nsw-government/about-website/copyright>

Contents

1	Introduction.....	3
1.1	Purpose.....	3
1.2	Scope.....	3
1.2.1	Exemption related to law enforcement matters.....	4
1.3	Out of scope.....	4
1.4	Policy framework.....	4
2	Policy Definitions	6
3	Australia's AI Ethics Principles	8
3.1	AI Ethics Principles summary	8
4	Agency requirements	9
5	Standard A: Accountability	10
5.1	Agency Head.....	10
5.2	Accountable Official.....	10
5.3	Governance Accountability	11
5.3.1	Overview	11
5.3.2	Governance Board accountabilities	11
5.4	Assurance Accountability.....	12
5.4.1	Overview	12
5.4.2	Assurance accountabilities.....	12
5.5	NSW Office for AI	13
5.6	NSW Government employees.....	14
6	Standard B: Acceptable Use	15
6.1	AI Usage Principles and practices	15
7	Compliance and reporting	17
7.1	Compliance with the policy	17
7.2	Attestation requirements.....	17
7.2.1	Exemptions pathway (first reporting period).....	17
7.3	Reporting AI related incidents.....	18
8	Supporting legislation and policy.....	19
9	Document control	21
9.1	Document Version History.....	21
9.2	Review date	21
10	Attachment A – AI Use Case registration.....	22
10.1	How registration works.....	22
10.2	Who must register	22
10.3	When and what to register	22
10.4	When the AI Assessment Framework applies.....	23

10.5 Intended outcomes	24
------------------------------	----

1 Introduction

1.1 Purpose

The NSW Artificial Intelligence (AI) Operational Policy (policy) sets out all-of-government requirements to support the safe, ethical and lawful use of AI within the NSW Government. It defines governance and assurance accountabilities and establishes mandatory rules for acceptable AI use that NSW Government agencies and employees must follow, improving transparency to support safe AI adoption, innovation, collaboration and reuse.

The policy replaces the NSW AI Ethics Policy and adopts Australia's AI Ethics Principles to ensure consistent national alignment.

The policy applies to Agency Heads, executives and anyone responsible for using, implementing, governing, assuring, or approving AI systems.

The NSW Office for AI within Digital NSW, a division of the Department of Customer Service, maintains this policy and associated guidance and tools published by the NSW Office for AI.

1.2 Scope

The NSW AI Operational Policy applies to all NSW Government sector agencies¹ and Statutory Authorities/Bodies and their employees as per DCS Circular DCS-2026-02. This includes Departments, executive agencies related to Departments and separate agencies.

It is recommended that Advisory Entities (including Boards and Committees), State Owned Corporations and subsidiaries of the NSW Government established under the Corporations Act apply Australia's AI Ethics Principles and the NSW AI Assessment Framework to support the safe and responsible implementation of AI.

This policy applies to AI systems used by the NSW Government. In practice, an AI system comprises the AI use case, supported by products, platforms, and underlying infrastructure used to generate AI outputs.

There is no universally accepted technical or legal definition of AI. For the purposes of this policy, AI is defined in accordance with the OECD definition of an AI system:

“An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.”²

This policy complements and strengthens, rather than duplicates, existing frameworks, legislation and practices relating to NSW Government agency use of AI. Where this policy is inconsistent with a statutory obligation, the statute prevails.

¹ The term 'NSW Government sector agencies' as defined in the *Government Sector Employment Act 2013*.

² OECD (2024), “Explanatory memorandum on the updated OECD definition of an AI system”, OECD Artificial Intelligence Papers, No. 8, OECD Publishing, Paris, <https://doi.org/10.1787/623da898-en>.

Agencies must apply this policy alongside existing obligations, including data, governance, cyber security, privacy and recordkeeping. Examples of relevant legislation and policies are included in **Section 9** of this policy.

On approval, the policy will be published on the Digital.NSW website and will replace the NSW AI Ethics Policy. The NSW Office for AI will identify opportunities to develop guidance and best practice examples to support consistent implementation.

Compliance with this policy is mandatory in accordance with DCS Circular DCS-2026-02 issued by the Department of Customer Service.

1.2.1 Exemption related to law enforcement matters

Law enforcement agencies are exempt from specific requirements of this policy to the extent that compliance would prejudice, or would be reasonably likely to prejudice, the agency's lawful performance of its operational, investigative, intelligence, protective or emergency response functions. This may apply in situations where compliance would compromise public safety, public order, security, or the confidentiality and effectiveness of covert, sensitive or classified activities. Any reliance by a law enforcement agency on this exemption must be strictly limited to what is necessary to avoid the prejudice.

This is not a blanket exemption, and it does not apply to administrative or non-operational uses of AI.

Agencies must ensure the terms of the exemption are documented with the NSW Office for AI and justified on a use-case basis, with periodic review to ensure that the exemption remains confined to what is reasonably necessary.

Agencies relying on this exemption must maintain strong internal governance and assurance, including clear accountability for AI oversight, internal review mechanisms, and continued application of Australia's AI Ethics Principles.

1.3 Out of scope

This policy is not mandatory for local government, universities or third-party suppliers.

This policy does not apply to standard automation and analytics that follow predefined logic and do not generate predictions or recommendations used to inform or automate decisions. This includes macros, scripts, deterministic rules-based processes, and descriptive analytics.

1.4 Policy framework

The NSW Government AI policy framework includes:

- **Australia's AI Ethics Principles** provides overarching national guidance to help ensure AI systems are safe, fair, transparent, accountable, and aligned with human and societal wellbeing.
- **The NSW AI Strategy** sets the direction on the development and use of AI by NSW Government agencies.
- **The NSW AI Operational Policy** sets mandatory requirements for AI governance, assurance and acceptable use. This policy replaces the NSW AI Ethics Policy and requires agencies to adhere to Australia's AI Ethics Principles.
- **AI Assessment Framework (AIAF)** is a mandatory risk assessment tool applied to AI use cases at defined points across the AI lifecycle and when changes to risk, context or system functionality could affect outcomes or oversight.
- **Agency-level policy and standards** may introduce additional requirements to the NSW AI Operational Policy based on the agency's size, use of AI and operating context, but they must not

change or remove any requirements set out in this policy. The NSW Office for AI can provide advice where there is uncertainty or if a conflict exists.

2 Policy Definitions

Term	Definition in this policy
Accountable Official	The Accountable Official is the designated senior executive within an agency responsible for overseeing implementation of the NSW AI Operational Policy within that agency.
Accountable Owner	The person with responsibility and decision-making authority for the AI use case, who is accountable for the accuracy and completeness of the AI Assessment Framework and for the outcomes arising from the AI use case.
Agency	Agency means the NSW government sector agencies within scope of this policy.
Agency Head	Agency Head means: • In the case of a Department, the Secretary of the Department, or • In any other case, the head of the agency within scope of this policy.
AI Assessment Framework (AIAF)	The AIAF is a mandatory risk assessment tool for NSW Government agencies to ensure responsible design, development, deployment, procurement and use of AI technologies. It supports agencies to assess AI risk, define required mitigations, and demonstrate alignment with the ethical principles.
AI Assessment Framework Platform	The AIAF Platform is the central system that operationalises the AIAF, enabling agencies to register AI use cases, assess risks, identify required controls, and share and reuse insights, supporting all-of-government visibility and agency-level risk insights.
AI incident³	An event, circumstance or series of events where the development, use or malfunction of one or more AI systems directly or indirectly leads to any of the following harms: • injury or harm to the health of a person or groups of people • disruption of the management and operation of critical infrastructure • violations of human rights or a significant breach of obligations under applicable laws, including intellectual property, privacy and Indigenous cultural and intellectual property • harm to property, communities or the environment.
AI platform	A shared technology environment that provides infrastructure and services to build, integrate, and operate AI products.
AI product	An application or system that provides AI capabilities which can be used across multiple use cases.
AI Review Committee	The NSW AI Review Committee (AIRC) brings together independent experts and public servants to review high risk AI systems, providing practical, risk-informed guidance to NSW Government agencies. The advice supports safe, lawful and responsible implementation. Agencies retain full decision-making authority and accountability when applying this advice.
AI system	OECD definition

³ Definition is consistent with the Australian Government's *Technical standard for government's use of artificial intelligence*.

Term	Definition in this policy
	An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment. Simple explanation An AI system is a system that uses data to generate predictions, content, recommendations or decisions that can influence outcomes. AI systems include the products, platforms, tools and underlying infrastructure used to deliver the system outcome.
AI system lifecycle	The AI system lifecycle covers all stages of an AI system, from concept/design, procurement, pilot/validation, deployment, operations and review/retirement.
AI use case	A specific application of an AI system for an intended purpose within a defined business, service, or operational context. A use case describes what the AI is being used to do, who it affects, what data, inputs and outputs are involved, and the decisions, actions, or outcomes it may influence.
Critical-risk	The AI system or application presents the highest level of risk. Impacts may be severe, widespread, or irreversible, requiring the strongest governance attention.
Data⁴	Data is a broad term, the definition of which is heavily impacted by context. Data generally refers to facts and figures that can be represented as numbers, text, graphics, sound or video, as well as how these are interpreted. Data can also take different forms e.g. digital and can pertain to a range of topics or areas e.g. people, systems and the environment. Data can further be broken down by type or purpose, for example transactional and operational data.
Department	Department means the departments listed in Part 1, Schedule 1 of the <i>Government Sector Employment Act 2013</i> .
Employee	Employee means a person employed in ongoing, term, temporary, casual or other employment, or on secondment in an agency listed within scope of this policy.
High-Risk	AI systems or applications that present a substantial risk profile. Impacts may be significant, affect trust or operations, and require close management and oversight.
Low-risk	AI systems or applications that, if they malfunction or produce unintended outcomes, can be easily reversed or corrected without causing any harm or damage.
Medium-risk	AI systems or applications that present a moderate level of risk. Impacts may be noticeable but are generally limited and manageable with proportionate effort.
Public AI tool	An AI-enabled product or service that is publicly available for general use, including tools accessed via the internet or third-party platforms, where the organisation does not control the underlying model, data processing, or system operation.
Responsible owners	The appropriate person, role or group within an agency that is accountable for ensuring an activity, task or program of work is delivered as intended.

⁴ Definition of data as outlined in the NSW Data Strategy.

3 Australia's AI Ethics Principles

This policy adopts Australia's AI Ethics Principles as the mandatory NSW Government AI ethical principles. The ethical principles guide the NSW Government to practice the highest ethical standards when using, designing, developing and implementing AI.

3.1 AI Ethics Principles summary ⁵

- **Human, societal and environmental wellbeing:** AI systems should benefit individuals, society and the environment.
- **Human-centred values:** AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness:** AI systems should be inclusive and accessible and should not involve or result in unfair discrimination against individuals, communities or groups.
- **Privacy protection and security:** AI systems should respect and uphold privacy rights and data protection and ensure the security of data.
- **Reliability and safety:** AI systems should reliably operate in accordance with their intended purpose.
- **Transparency and explainability:** There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI and can find out when an AI system is engaging with them.
- **Contestability:** When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- **Accountability:** People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

⁵ For further information on each principle please refer to Australia's AI Ethics Principles: <https://www.industry.gov.au/publications/australias-ai-ethics-principles>, Department of Industry, Science and Resources

4 Agency requirements

This policy provides flexibility for agencies to determine the appropriate approach to implementing the mandatory requirements considering their operating context, size, and functions.

The **mandatory requirements** are:

1. Adhere to Australia's AI Ethics Principles when using, designing, developing, deploying and implementing AI systems. Agencies should use AI in ways that benefit individuals, society and the environment.
2. Designate an Accountable Official (Senior Executive) who is nominated by the Agency Head to oversee implementation of the NSW AI Operational Policy in that agency and notify the NSW Office for AI within three months of this policy being issued.
3. Ensure your agency AI governance and assurance functions comply with Standard A: Accountability.
4. Ensure your Information Communications Technology (ICT) acceptable use policy and guidance comply with Standard B: Acceptable Use.
5. Register all AI use cases in the AIAF Platform and maintain accurate and complete records across the AI system lifecycle. Agencies may use their own systems but must synchronise records to the AIAF Platform.
6. Apply the AIAF to an AI use case where the registration process determines an assessment is required. Any critical-risk and high-risk AI use cases must be referred to the AI Review Committee for advice on risk management.
7. Ensure that basic AI literacy training and relevant policy training modules are made available to employees who use AI, or whose roles involve the development, procurement, management, assurance, or approval of AI systems. The NSW Office for AI will provide the training modules. Agencies with existing training must demonstrate alignment with these modules and seek an exemption from the NSW Office for AI.

5 Standard A: Accountability

5.1 Agency Head

The Agency Head is accountable for:

- Nominating an Accountable Official to oversee implementation of the policy in that agency.
- Ensuring the agency complies with the policy and its requirements.
- Approving and signing an annual attestation of compliance with the policy, to be submitted to the NSW Office for AI.

The Agency Head may designate an Accountable Official from ICT, business, policy, procurement, governance or other areas of the agency depending on the agencies size, structure and capability. In practice, the Secretary of a department may appoint one Accountable Official for that department or nominate separate Accountable Officials for each agency within that department. Agencies that operate independently of their department governance and assurance arrangements must appoint their own Accountable Official and implement the requirements of this policy.

The Accountable Official must be a senior executive with the authority and influence to effectively drive the policy's implementation for that agency.

5.2 Accountable Official

The Accountable Official is accountable for overseeing the implementation of the policy within their agency. This includes:

- Ensuring governance and assurance oversight of AI is aligned with existing governance arrangements, or establishing appropriate governance where it does not exist or is not sufficient.
- Ensuring responsible owners understand and communicate the agency's AI use case registration process to relevant employees.
- Ensuring responsible owners align the agency's ICT Acceptable Use policy with Standard B of this policy.
- Ensuring responsible owners make AI literacy and policy training modules available to relevant employees.
- Notifying the NSW Office for AI of any suspected or confirmed AI incidents and coordinating AI use cases for post-incident review to the AI Review Committee when needed.
- Preparing and endorsing the agency's annual attestation, to be signed by the Agency Head and submitted to the NSW Office for AI by 31 October each year.
- Acting as the agency's point of contact for all-of-government AI policy coordination.
- Notifying the NSW Office for AI of the appointment of the Accountable Official, and of any changes to the appointment, via email to oi@customerservice.nsw.gov.au.

5.3 Governance Accountability

5.3.1 Overview

This section outlines the baseline governance accountabilities for an agency's governance board to ensure the safe, lawful and ethical use of AI. Agencies may establish additional governance accountabilities where appropriate to their context.

Agencies have flexibility in how these requirements are implemented within their operating context and should consider:

- Leveraging existing governance boards or functions with responsibility for operational risk, and/or expanding boards or functions that oversee digital initiatives to include AI oversight.
- Agency size and operational context, including the scale and complexity of AI use.
- The agency's existing governance maturity and remit.
- Ensuring governance board membership includes executive-level roles with appropriate authority.
- Establishing a working group or sub-committee to provide expert advice to the governance board, where appropriate. This group may include members with a mix of expertise such as legal, policy, ethics, data, privacy, cyber, human resources, and AI, to support the identification, assessment, and oversight of AI related risks.

Ultimately, each agency is responsible for determining how best to embed AI oversight and risk management within its governance arrangements.

Where implementation of AI may result in workforce impacts, agencies should use existing workforce consultation and organisational change processes in line with relevant employment and industrial obligations.

5.3.2 Governance Board accountabilities

The Accountable Official **must** ensure there is an existing **governance** board (or boards) responsible for AI oversight or establish appropriate arrangements where none exist. The governance board remains accountable for these requirements, with implementation undertaken by appropriate governance, risk, or assurance functions.

The governance board is accountable for:

- a. **Registration and assessment:** Confirm that AI use cases are registered in the AIAF Platform and that an AIAF assessment is completed when required.
- b. **AI Review Committee referral:** Refer all critical risk and high-risk AI use cases to the AI Review Committee (AIRC) by notifying the Secretariat within five business days of completing the AIAF by email at AIsecretariat@customerservice.nsw.gov.au. Ensure all AIRC recommendations are implemented or a documented, justified rationale is maintained.
- c. **Risk oversight:** Approve the level of governance oversight required for each AI use case, ensuring it is proportionate to the risk band determined through the AIAF assessment.
- d. **Decision making:** Ensure decision-makers of AI systems consider human, societal and environmental impacts across the AI system lifecycle, including appropriate Aboriginal and Torres Strait Islander representation in design, implementation and oversight.
- e. **Audit and review:** Ensure teams have plans to review AI systems at a frequency appropriate to their risk band and that annual audits are conducted for high-risk and critical-risk AI uses.
- f. **Service continuity:** Ensure AI dependencies supporting critical services have tested business continuity plans that can be activated when required.

- g. **Transparency:** Ensure the agency proactively discloses and explains where an AI system is used to inform, support or automate decisions that may impact a person's rights, interests, or access to services.
- h. **Appeal and redress:** Ensure AI systems provide clear, accessible information about appeal mechanisms, enabling people to challenge and seek remedies for AI-enabled decisions that affect their rights and interests, or that may significantly impact communities or the environment.
- i. **Alternative channels:** Where AI interacts with the public, ensure a human or non-AI service option is available as part of the overall service.
- j. **Escalation pathways:** Ensure clear mechanisms are in place for employees to report non-compliance with this policy and AI incidents to the governance board, including raising concerns related to their work, responsibilities, or broader AI safety issues.
- k. **Oversight effectiveness:** Annually review the effectiveness of the agency's AI governance and assurance functions, report outcomes to the Agency Head, and implement improvements to ensure these functions remain fit for purpose.

5.4 Assurance Accountability

5.4.1 Overview

This section sets out the baseline accountabilities for an agency's assurance function. Agencies may introduce additional accountabilities where appropriate and have flexibility in how these requirements are implemented within their operating context.

Agencies should consider:

- Using existing functions with responsibility for project, program, or operational assurance.
- Agency size and operational context, including the scale and complexity of AI use.
- The agency's existing assurance maturity and remit.
- Ensuring assurance functions include director-level roles, with appropriate expertise in AI risk and system operation, to assess the effectiveness of controls and verify compliance.

Ultimately, each agency determines how AI assurance is embedded within its organisational arrangements.

5.4.2 Assurance accountabilities

The Accountable Official **must** oversee the establishment of an assurance function, or functions, accountable for the following:

- a. **System accountability:** Confirm that there is a clearly identified and documented Accountable Owner for each AI system.
- b. **Registration and assessment:** Ensure all AI use cases are registered and appropriately documented in the AIAF Platform, and that the AIAF is applied when required.⁶
- c. **Risk band:** Approve the intrinsic risk band for each AI use case assessed under the AIAF, ensuring it aligns with the assessment outcomes.

⁶ The AIAF Platform registration process determines whether an assessment is required. Guidance on registration, documentation, and assessment is available on the Digital NSW website.

- d. **Reassess Risks:** Ensure AI risks are reassessed across the AI system lifecycle, including when changes to risk, context or system functionality could affect outcomes or oversight.
- e. **Monitoring:** Ensure the Accountable Owner monitors medium-risk, high-risk and critical-risk AI systems across the lifecycle to confirm they operate as intended, with appropriate human oversight. Monitoring responsibilities must be clearly assigned and documented.
- f. **Management of third-party supplier risks:** Ensure third-party risks are identified and managed by the Accountable Owner, including where AI systems rely on shared ICT services supplied by other NSW Government agencies. Contractual arrangements must support transparency, including mechanisms for suppliers to disclose AI use and notify the agency of material changes over time.
- g. **Incident response:** Ensure high-risk and critical-risk AI use cases have incident response plans, human override mechanisms, and clear appeal pathways.
- h. **Benefit review:** Ensure post-implementation reviews are undertaken to assess the effectiveness, performance, and safety of AI systems in real world settings.
- i. **Recordkeeping:** Ensure accurate and complete records are captured and retain across the AI system lifecycle, including AI outputs and metadata where they inform decisions, are relied on in official processes, or may be subject to review, audit, or challenge. Records must be managed as State records in accordance with the *State Records Act 1998*.
- j. **Continuity and sovereign capability:** Ensure AI systems are designed and implemented to maintain continuity of government services, including the ability to operate or transition services if an AI solution, model or service becomes unavailable or materially changes.

5.5 NSW Office for AI

The NSW Office for AI is responsible for all-of-government AI policy and guidance. This includes supporting capability uplift to accelerate the safe adoption of AI, enabling knowledge sharing to reduce duplication, and leading the transition to an AI-enabled NSW Government.

The NSW Office for AI will support agencies to meet the NSW AI Operational Policy requirements by providing related guidance, templates, developing AI literacy and policy training courses in collaboration with TAFE NSW, and developing and onboarding agencies to the AIAF Platform.

The NSW Office for AI accountabilities include:

- a. **Policy & Standards:** Set, maintain, and update the NSW AI Operational Policy and related guidance to reflect emerging technologies, evolving risks, and legislative changes.
- b. **Capability Support:** Provide agencies with guidance, training modules, tools, and ongoing advice to support implementation of this policy. Collect and analyse agency reporting on AI literacy and policy module training completion, pass rates, and participant feedback to inform training improvements. Operate the AIAF Platform and support agencies to complete or synchronise AIAF assessments through the platform.
- c. **High-Risk Oversight:** Maintain all-of-government visibility of high-risk and critical-risk AI use cases and coordinate referrals to the AI Review Committee (AIRC) for advice on risk mitigation. The NSW Office for AI may also refer medium-risk AI use cases to the AIRC where higher risk characteristics are present.
- d. **Transparency & Collaboration:** Identify cross-agency issues and opportunities for coordinated action to strengthen accountability, improve acceptable use practices, and increase public transparency of government AI use.
- e. **Reporting and escalation:** Report annually to the NSW Secretaries Board using AIAF data to highlight AI use trends, risks, and opportunities across the NSW Government. Refer reported AI incidents to the AIRC for post-incident review and expert advice where required.

- f. **Policy Alignment:** Align NSW all-of-government AI policy and guidance with Commonwealth policy developments and evolving national and international AI standards.
-

5.6 NSW Government employees

NSW Government agency employees are accountable for the following:

- a. **Permitted use:** Use AI in alignment with agency ICT Acceptable Use Policies and guidance.
- b. **Transparency and risk assessment:** Follow agency policies and processes related to registration of AI use cases in the AIAF Platform and completion of the AIAF.
- c. **Report issues:** Escalate any concerns of non-compliance with this policy, AI incidents, or broader AI safety issues in accordance with agency governance and escalation processes.

6 Standard B: Acceptable Use

This section establishes the mandatory AI usage principles and practices for NSW Government employees to ensure AI is used safely, responsibly and ethically. Agencies must update their ICT Acceptable Use Policy to align with these mandatory requirements to ensure consistent local application.

Employees must follow their agency's ICT acceptable use policies, guidance and approved controls when using AI. These agency instruments are the primary mechanisms through which Standard B is implemented and must align with the principles and practices set out below. Where an agency applies stricter controls, those controls prevail.

6.1 AI Usage Principles and practices

NSW Government agencies and employees must comply with the following principles and practices when using AI.

An AI system is a system that uses data to generate predictions, content, recommendations or decisions that can influence outcomes. AI systems include the products, platforms, tools and underlying infrastructure used to deliver the system outcome.

1. Safeguard government information

- Treat all inputs to and outputs of AI systems as potentially shared with the provider.
- Do not enter personal and/or health information⁷ (OFFICIAL: Sensitive or above)⁸ or security classified information into AI systems unless this use is explicitly approved by your agency.
- Do not activate AI features, plugins, or integrations within agency systems unless explicitly approved.

2. Ensure meaningful human oversight

- Treat AI outputs as advisory and do not rely on them as the sole basis for decisions. Apply greater oversight for higher-risk decisions and retain human judgement.
- Ensure an authorised human decision-maker reviews any outputs of an AI system that are used to inform or make decisions affecting a person's rights or interests, or access to services.
- Apply human oversight and strict controls where AI systems can plan, decide or act autonomously.⁹

3. Remain responsible and accountable for your AI use

- Be accountable for any you create, use, or share that is generated wholly or partially by AI. You must be able to explain and justify its use and any decisions informed by it.
- Clearly disclose AI-generated content where it may be used in critical decision-making processes or may affect people's rights, interests, access to services, or trust in the NSW Government. Provide a level of disclosure appropriate to the audience and context.

⁷ Refer to the definitions of 'personal information' and 'health information' as set out in the *Privacy and Personal Information Protection Act 1998* and *Health Records and Information Privacy Act 2002*.

⁸ NSW uses six Dissemination Limiting Markers (DLM) to describe the type of sensitivity of the information. Refer to the [NSW Government Information Classification, Labelling and Handling Guidelines](#) for definitions.

⁹ Refer to the '[AI agent usage and deployment guidance](#)' for NSW Government agencies published on the [digital.nsw](#) website.

- Ensure complete and accurate records of AI-generated decisions, insights, or content are captured and retained as State records, where they inform or support decisions that may affect people's rights, interests, or access to services.¹⁰
- Ensure AI-generated content used in official corporate, strategic and marketing communications is reviewed and approved in line with agency communication guidelines.

4. Critically assess AI outputs to verify quality and accuracy

- Verify AI outputs before use and on an ongoing basis, applying professional judgement to assess accuracy, fairness, bias, and ensure outputs are not misleading or presented with undue certainty.
- Ensure AI outputs are appropriate for diverse communities, including Aboriginal and Torres Strait Islander people, and meet accessibility requirements.
- Complete required AI literacy and policy training modules made available in your agency to support safe, lawful and ethical use of AI.
- Consider whether AI use may create risks to the health, safety or wellbeing of employees, and take appropriate action, including reporting concerns.
- Report suspected or actual unsafe, biased, or harmful AI use through your agency governance and escalation processes.

5. Adhere to legislation, policy and ethics

- Ensure your use of AI supports public trust and upholds government sector core values and complies with the Ethical Framework and the Code of Ethics and Conduct for NSW Government Sector Employees.
- Ensure your use of AI is consistent with Australia's AI Ethics Principles and relevant NSW Government and agency AI policies.
- Staff who use, design, develop, implement and approve AI systems must comply with relevant laws, policies, and standards, including legislation under which the AI system operates.

¹⁰ Understand and meet your obligations under the *State Records Act 1998* for records created across the AI system lifecycle, including AI generated content and metadata. Refer to the AI and recordkeeping guidance for further information.

7 Compliance and reporting

7.1 Compliance with the policy

Agencies will have a transitional period from the time the policy is issued to implement the policy requirements. The NSW Office for AI will issue an implementation guide to support this process. Agencies should notify the NSW Office for AI where they lack the resources and expertise to implement the governance and assurance of AI.

The NSW Office for AI strongly recommends that agencies consider incorporating compliance with this policy into existing audit, risk and assurance programs, including internal audit plans and governance, risk and compliance processes, to provide ongoing independent assurance.

An agency's AI governance board is required to establish clear pathways for employees to report non-compliance with this policy to the governance board. The agency should seek to remedy the non-compliance and where it cannot be remedied, the AI governance board should notify the Agency Head and Accountable Official. The Accountable Official must detail any non-compliance in the agency's attestation to the NSW Office for AI.

The NSW Office for AI may use AIAF Platform data and attestation reporting to identify areas of risk and work with agencies to prioritise activities. The NSW Office for AI may refer all-of-government risks to the NSW Secretaries Board for visibility and to make decisions to support safe and responsible AI adoption.

7.2 Attestation requirements

Agencies must provide a signed annual attestation for the previous financial year to the NSW Office for AI by 31 October each year, commencing with the first reporting date of 31 October 2027. This provides a minimum of 12 months for agencies to implement this policy from the time the policy is issued. The attestation process will form part of existing reporting requirements to Digital NSW, Department of Customer Service.

Where an attestation covers more than one agency, the attestation must include a list of all agencies covered. Where an attestation is submitted by a department, the attestation must also identify any agencies within that department that are not covered.

The Accountable Official must use the approved NSW Office for AI template to submit the signed annual attestation to the NSW Office for AI. The template includes the evidence requirements that address an agency's compliance with this policy.

The attestation must be endorsed by the Accountable Official and approved by the Agency Head prior to being submitted to the NSW Office for AI.

7.2.1 Exemptions pathway (first reporting period)

Some agencies may require additional time to meet the requirements of this policy for the first reporting period due to complex ICT environments, dependencies, or the scale of implementation. To support a risk-based and practical transition, an agency may request an extension to the first annual attestation.

An extension request must:

- a. be submitted by the Accountable Official and endorsed by the Agency Head,
- b. describe which requirements cannot be met by the first attestation date and why. For example, complex systems integration, procurement lead times, resourcing constraints,
- c. provide a time-bound remediation plan, including milestones, interim controls to manage risk, and a target date for achieving compliance.

The NSW Office for AI will review extension requests to ensure they are complete, accurate, and sufficiently detailed, and that they clearly describe the requirements not met, the reasons, and a time-bound remediation plan with appropriate interim controls. The NSW Office for AI will also confirm that the request and supporting information have been recorded in the agency's record management system in accordance with recordkeeping obligations, to support accountability and auditability.

Requests must be made in writing to the NSW Office for AI via oai@customerservice.nsw.gov.au prior to 30 September of every reporting year.

7.3 Reporting AI related incidents

The agency AI governance board must ensure clear escalation pathways are established to enable employees to report AI incidents and raise concerns about AI use related to their work, responsibilities or broader AI safety matters. Examples of AI incidents include sensitive data breaches, misleading outputs used in decisions, biased or unfair outcomes, unauthorised use of AI systems, and AI systems generating harmful or unreliable content.

The AI governance board is responsible for deciding whether an incident reported to them constitutes an AI incident and may contact the NSW Office for AI for advice if unsure. The AI governance board must report AI incidents to the Accountable Official, who is responsible for notifying the NSW Office for AI of the incident via email at oai@customerservice.nsw.gov.au. The NSW Office for AI will work with the Accountable Official to refer the AI incident to the AI Review Committee (AIRC) for post-incident review and advice.

In the event of a cyber security incident relating to an AI system, agencies must follow their incident management procedures, including reporting cyber incidents to Cyber Security NSW as required under the [NSW Cyber Security Policy](#). Cyber Security NSW will notify the NSW Office for AI where a cyber security incident relates to an AI system for visibility. In these cases, the NSW Office for AI will work with the Accountable Official of that agency to seek a post-incident review from the AIRC relating to the AI system.

Where a data breach is caused by an AI system or as a result of an AI incident, agencies must comply with the reporting requirements under the [NSW Mandatory Notification of Data Breach Scheme](#) which requires impacted agencies to notify the Privacy Commissioner and provide notifications to affected individuals in the event of an eligible data breach.¹¹ The agency Senior Responsible Officer for records management must report data breaches to State Records NSW where data/information/records have been damaged, lost or destroyed.¹²

¹¹ Part 6A of the *Privacy and Personal Information Protection Act 1998* (NSW) establishes the NSW Mandatory Notification of Data Breach Scheme.

¹² For further information about the steps to notify State Records NSW visit the [nsw.gov.au](https://www.nsw.gov.au/nsw-government/recordkeeping/notification-damaged-records) website here: <https://www.nsw.gov.au/nsw-government/recordkeeping/notification-damaged-records>.

8 Supporting legislation and policy

This section sets out AI related legislation and policy. The below list is not exhaustive, and agencies must consider which existing legislative, policy and other requirements apply to them and their specific AI use case.

Access to information

- [Government Information \(Public Access\) Act 2009](#)

Cybersecurity

- [NSW Cyber Security Policy](#)

Data

- [NSW Government Information Classification, Labelling and Handling Guidelines](#)
- [Protective Security Policy Framework \(2025\)](#)
- [NSW Mandatory Notification of Data Breach Scheme](#)

NSW Government employment

- [Government Sector Employment Act 2013](#)

Privacy

- [Privacy Act 1988 \(Cth\)](#)
- [Privacy and Personal Information Protection Act 1998 \(NSW\)](#)
- [Health Records and Information Privacy Act 2002 \(NSW\)](#)
- [NSW Mandatory Notification of Data Breach Scheme](#)

Procurement

- [Procurement Policy Framework \(December 2024\)](#)
- [Public Works and Procurement Act 1912 No 45](#)

Recordkeeping

- [State Records Act 1998 \(NSW\)](#)
- [State Records Regulation 2024 \(NSW\)](#)

Rights and inclusion

- [Age Discrimination Act 2004](#)
- [Disability Discrimination Act 1992](#)
- [Racial Discrimination Act 1975](#)
- [Sex Discrimination Act 1984](#)
- [Australian Human Rights Commission Act 1986](#)
- [Anti-Discrimination Act 1977 \(NSW\)](#)
- [Disability Inclusion Act 2014 \(NSW\)](#)
- [AS EN 301 549: Accessibility requirements for ICT products and services](#)
- [AS EN 17161: Design for All - Accessibility following a Design for All approach in products, goods and services](#)

- The Ethical Framework and the Code of Ethics and Conduct for NSW Government Sector Employees

Work, health and safety

- Work Health and Safety Act 2011 (NSW)

9 Document control

9.1 Document Version History

Version	Status	Date	Prepared By	Comments
Final 1.0	Approved	11 June 2026	NSW Office for AI	Approved by the NSW Government Secretaries Board.

9.2 Review date

The NSW Office for AI will review this policy on an ongoing basis with additional revisions undertaken as necessary in response to emerging needs, technological changes and post-implementation feedback from NSW Government agencies.

The NSW Office for AI will continue to engage with departmental representatives responsible for AI governance and assurance, and/or the ICT and Digital Leadership Group (IDLG) to address implementation issues and inform future consultation processes.

A formal review will be undertaken on a 12-month cycle.

The IDLG are responsible for endorsing the NSW AI Operational Policy and any substantial updates, such as updates to mandatory requirements, without requiring Cabinet approval.

10 Attachment A – AI Use Case registration

An AI use case is a specific application of an AI system for an intended purpose within a defined business, service, or operational context. A use case describes what the AI is being used to do, who it affects, what data, inputs and outputs are involved, and the decisions, actions, or outcomes it may influence.

This section sets out:

- How AI use cases are registered and who is responsible
- Which AI use cases must be registered and when
- When the AI Assessment Framework applies
- The intended outcomes of registration and ongoing oversight

10.1 How registration works

AI use cases are registered through the AI Assessment Framework Platform.

Registration involves providing a minimum set of information about the AI use case and answering a short set of questions that determine whether an AI Assessment Framework (AIAF) assessment is required.

10.2 Who must register

There must be a clearly documented Accountable Owner responsible for ensuring that the AI use case is registered and for the accuracy and completeness of the AIAF assessment and outcomes arising from the AI use case.

Each AI use case must be registered once by the Accountable Owner at the:

- Agency level – where the use case is implemented as a shared or enterprise capability.
- Team level – where the use case is embedded in a team workflow or process.
- Individual level – where the use case is created and used independently.

10.3 When and what to register

When to register

AI use cases must be registered before use. Registration determines whether an AIAF assessment is required.

If AI is already in use, registration must occur as soon as practicable. Remaining use cases should be registered progressively as part of AI system governance, change management, or review cycles.

What to register

AI use cases must be registered where the use of AI introduces elevated risk, significant operational reliance, or impacts people, decisions, services, or includes use of personal and sensitive information. This includes:

- Where AI is used to automate or materially influence consequential decisions,
- AI embedded into operational workflows, systems, or public-facing services,
- Autonomous or semi-autonomous AI interactions, and
- Uses involving highly sensitive or security-classified information beyond approved purposes.

Routine productivity, analytical assistance, drafting, summarisation, coding support, and exploratory use of approved agency AI systems, platforms and products do not generally require registration where meaningful human oversight is maintained, and the use remains within approved agency guardrails.

The registration process includes the following baseline questions. These will be tested and implemented within the AIAF platform and will evolve over time to ensure AI use cases are identified and captured effectively as AI technology and its use continue to evolve.

- **Approved Tool** – Are you using an agency-approved AI system, platform or product?
- **Consequential Decision-Making** – Is the AI being used to automate or materially influence decisions that affect a person's rights, entitlements, access to services, compliance outcomes, or other consequential decisions?
- **Elevated-Risk Use** – Is the AI being used in a way that introduces elevated risk beyond routine productivity or analytical assistance?
- **Experimental Use** – Is the AI being used only for experimentation with synthetic, publicly available or non-sensitive information in an isolated environment, without informing real decisions, services or operational processes?

Precautionary approach

If unsure, take a precautionary approach and start the registration process. The platform will guide you and confirm whether further information or assessment is required.

Exclusions

The requirement to register AI use cases does not apply to third-party suppliers providing services to the NSW Government where they use AI as part of those services. These arrangements are managed through procurement, contracting, and supplier assurance processes.

10.4 When the AI Assessment Framework applies

The AIAF is a mandatory risk assessment tool for NSW Government agencies to ensure responsible design, development, deployment, procurement and use of AI technologies. It supports agencies to assess AI risk, define required mitigations, and demonstrate alignment with the ethical principles.

Registration in the AIAF Platform uses a rules-based approach to determine whether an AIAF assessment is required.

The AIAF applies at the AI use case level. It assesses the purpose, operational context, data involved, and downstream impact of specific AI uses.

It must be applied at defined points across the AI system lifecycle, and whenever risks, context or system functions change in ways that could affect outcomes or oversight. Key project phases are defined in the AIAF.

The AI use case should be re-assessed again where there are any material changes in purpose, data, decision context, or risk profile.

The AIAF applies an intrinsic risk assessment approach. Intrinsic risk characterises the risk of an AI use case as a function of what the use case involves and how it is intended to be used, rather than how it may later be managed or mitigated. The intrinsic risk band determines the minimum governance and oversight requirements for the AI use case.

Roles and responsibilities

The Accountable Owner is responsible for ensuring that the AI use case is registered and for the accuracy and completeness of the AIAF assessment, outcomes arising from the AI use case, and ongoing risk management.

Subject matter expert (SME) review under the AIAF provides assurance that assessment answers accurately reflect the actual use case, and that the resulting risk band is plausible given the information provided.

No SME review under the AIAF:

- approves or rejects AI use cases
- certifies legal compliance
- authorises deployment
- accepts organisational risk.

The AI governance function within an agency approves the level of oversight of the AI use case and ensures that the agency's AI use is aligned to strategic, policy, and ethics requirements. The assurance function is responsible for ensuring that risks relating to the agency's AI use are identified and managed effectively and that AI systems controls and processes are in place and functioning as intended.

10.5 Intended outcomes

Adoption of a centralised AIAF Platform is expected to deliver the following outcomes:

- Clarifies when the AIAF applies, provided through the deterministic registration step.
- Supports agencies apply proportionate governance, with AIAF review effort calibrated to operational risk, not platform adoption.
- Enables evidence-based oversight of AI use within an agency and across NSW Government agencies.
- Surfaces common AI use patterns to enable targeted guidance and agency level insights.
- Enables agencies to identify and connect with others working on similar use cases.
- Supports knowledge sharing and reuse of proven approaches.
- Enables continuous improvement through agency insights to inform updates to policies, guidance and to strengthen the AIAF over time.

